Charakterystyka rozpoznania w operacji typu COIN

Krzysztof Danielewicz

Security in practice

ISSN: 2719-9282

Charakterystyka rozpoznania w operacji typu COIN

Opracował: dr Krzysztof Danielewicz

Artykuł oryginalnie ukazał się w:*Charakterystyka rozpoznania w operacji typu COIN*, w: „Bezpieczeństwo Teoria i Praktyka", Czasopismo Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, nr 1(VI), Kraków 2012, s. 45–63

W związku z ostatnimi konfliktami zbrojnymi, a szczególnie tymi w Iraku i Afganistanie, jasno widać, że zasadniczo zmieniła się rola rozpoznania. We wcześniejszych, konwencjonalnych konfliktach rola rozpoznania zaczynała się na długo przed wybuchem samego konfliktu i polegała głównie na ustaleniu struktury organizacyjnej wojsk przeciwnika, jego wyposażenia, wyszkolenia oraz lokalizacji jego pododdziałów. Rozpoznanie było oparte głównie na technicznych środkach rozpoznawczych. W trakcie trwania konfliktu koncentrowano się na określeniu położenia i zamiaru działania przeciwnika. Wcześniej rozpoznana taktyka działania, zasadniczo nie zmieniała się w trakcie samego konfliktu. Różne bataliony czy brygady były podobnie ukompletowane i wyszkolone.

Większość armii na świecie nadal opiera posiadany system rozpoznawczy na założeniach wojny konwencjonalnej. Nawet w przypadku USA niektóre brygady wysłane do Iraku w początkowym okresie konfliktu musiały na miejscu dostosowywać swój system rozpoznawczy do nowych, nieznanych im warunków konfliktu asymetrycznego.

Niniejszy artykuł jest próbą ukazania miejsca i roli rozpoznania w operacji zbrojnej typu COIN (od angielskiego słowa „counterinsurgency" – działania przeciwpartyzanckie). Dodatkowo autor scharakteryzował podstawowe źródła informacji oraz przedstawił zasadnicze różnice w funkcjonowaniu rozpoznania w konflikcie typu COIN i konflikcie konwencjonalnym. Intencją autora było także scharakteryzowanie najbardziej efektywnych sposobów uzyskiwania informacji rozpoznawczych, a także problemów występujących w trakcie ich analizy.

Skuteczne rozpoznanie jest warunkiem kluczowym prowadzenia każdego rodzaju działań zbrojnych. W większości krajów na świecie funkcjonujące systemy zbierania i analizowania informacji rozpoznawczych są przygotowane do prowadzenia wojny konwencjonalnej. W konsekwencji, w przypadku udziału w operacji typu COIN, przed komórkami odpowiedzialnymi za prowadzenie rozpoznania stoją bardzo trudne, nie zawsze możliwe do

zrealizowania, zadania. Funkcją rozpoznania w COIN jest posiadanie aktualnej wiedzy na temat ludności lokalnej, środowiska operacyjnego oraz przeciwnika.

Zanim przejdziemy do szczegółowego omówienia roli rozpoznania w operacji typu COIN, ważne jest zrozumienie różnicy między pojęciami „counterinsurgency" a „counterguerrilla". Według słownika języka angielskiego „insurgency" to powstanie (powstańcy), natomiast „guerrilla" to partyzantka[1]. Na podstawie prostego tłumaczenia tych pojęć na język polski trudno byłoby zdefiniować różnicę w operacji skierowanej przeciw (counter) partyzantom i powstańcom[2].

W aktualnie obowiązującej nomenklaturze sojuszniczej operacja typu COIN skierowana jest zarówno do powstańców, jak i lokalnej ludności. Jej głównym celem jest neutralizacja warunków mogących powodować lub sprzyjać rozwojowi ruchów powstańczych[3]. W operacji COIN uwzględniane są także takie elementy, jak: rozwój gospodarczy, inwestycje w naukę, rozwój demokracji poprzez promocję instytucji demokratycznych i inne mające na celu przekonanie lokalnej ludności do poparcia sił COIN.

COIN można także zdefiniować jako operację wojskową, psychologiczną, ekonomiczną oraz cywilną podjętą przez rząd lub funkcjonujące władze w celu zwalczenia ruchu powstańczego[4].

Insurgency oraz stosowana przez nich taktyka jest stara jak sama wojna. Insurgency możemy zdefiniować jako zorganizowany ruch, którego celem jest obalenie konstytucyjnego rządu poprzez działania zbrojne, zamachy, sabotaż oraz inne, mające doprowadzić do osiągnięcia zamierzonego celu. Można go także określić jako zorganizowaną polityczno-militarną opozycję działającą w celu osłabienia kontroli i legalności funkcjonującego rządu, władzy okupacyjnej lub innej, jednocześnie wzmacniając swoją pozycję[5]. W strukturze organizacyjnej sił insurgency można wyróżnić pięć podstawowych elementów: liderzy ruchu, aktywnie walczący członkowie (główne, regionalne i lokalne siły), kadry polityczne, aktywni zwolennicy/sympatycy zapewniający istotne wsparcie logistyczne oraz masy potencjalnych zwolenników[6].

Władza polityczna jest kluczowa zarówno dla powstańców, jak i sił COIN. Obie strony, walcząc o serca i umysły ludności cywilnej, dążą do przekonania jej o zasadności i legalności swoich rządów czy władzy. Powstańcy dla realizacji swojego celu używają wszelkich możliwych sił i środków: politycznych (włącznie z dyplomatycznymi), informacyjno-propagandowych (odwołując się do religii, etyki czy ideologii), militarnych i ekonomicznych[7].

W przypadku operacji typu counterguerrilla jest ona ukierunkowana na zwalczanie tylko elementów zbrojnych (partyzantów) i jest częścią wspierającą operacje typu COIN jako całość[8].

W przypadku wojny konwencjonalnej ryzyko utraty suwerenności przez jedno z państw jest duże, jednak ryzyko wystąpienia takiego konfliktu – małe. W przypadku COIN ryzyko utraty suwerenności przez państwo zaangażowane jest niewielkie, natomiast częstotliwość tego typu konfliktów jest w dzisiejszych czasach duża. W konfliktach konwencjonalnych dochodzi do starcia regularnych armii. Operacje COIN charakteryzują się występowaniem opozycji zbrojnej wewnątrz państwa, wspieranej częstokroć przez wrogie czynniki zewnętrzne. W historii wielokrotnie mieliśmy także do czynienia z jednoczesnym występowaniem konfliktów konwencjonalnych i niekonwencjonalnych. W trakcie drugiej wojny światowej Niemcy

niejednokrotnie zmuszone były prowadzić jednocześnie działania regularne i przeciwpartyzanckie – counterguerrilla[9].

ZNACZENIE ROZPOZNANIA W COIN

Wyznacznikiem sukcesu w operacji COIN nie jest liczba zniszczonych mostów i budynków, spalonych samochodów czy też liczba zabitych członków opozycji – jak to ma miejsce w wojnie konwencjonalnej. Głównym kryterium efektywności jest zniszczenie lub znaczne ograniczenie skuteczności wysiłków przeciwnika i jego możliwości wykorzystania ludności lokalnej dla własnych celów[10].

Niezwykle istotne jest zrozumienie otoczenia COIN oraz różnic występujących pomiędzy operacją COIN a innymi rodzajami operacji. Prawidłowe zrozumienie zasad panujących w otoczeniu COIN pozwoli na odpowiednią alokację posiadanych środków rozpoznawczych.

Na podstawie praktycznych doświadczeń zebranych w trakcie ostatnich konfliktów nieregularnych można wyodrębnić sześć charakterystyk, które odróżniają COIN od innych operacji zbrojnych[11]:

1. **Rozpoznanie w COIN dotyczy ludzi** (rzecz najważniejsza). Dowódca na teatrze działań musi rozumieć lokalną ludność, zależności występujące w strukturach państwa gospodarza, ludzi przystępujących do zbrojnej opozycji, ich motywację oraz czynniki powodujące i sprzyjające rozwojowi sił insurgency. Bardzo ważne na tym etapie jest rozumienie systemu wierzeń i zależności występujących w społeczeństwie oraz sposób podejmowania decyzji.
2. **COIN jest wojną informacyjną oraz wojną systemów rozpoznawczych**. Zarówno insurgent, jak i counterinsurgentspotrzebują efektywnego rozpoznania. Kluczem do sukcesu w tym przypadku jest zorganizowanie sprawnego systemu pozyskiwania i opracowywania informacji oraz neutralizacja zdolności rozpoznawczych strony przeciwnej.
3. **Występuje ścisły związek pomiędzy prowadzonymi operacjami na teatrze a pozyskanymi informacjami o przeciwniku.** W operacji COIN rozpoznanie i operacje są od siebie uzależnione w sposób bardzo dynamiczny. Dzięki wiarygodnym informacjom można prowadzić skuteczne operacje, które pozwalają uzyskać kolejne istotne informacje rozpoznawcze. Złe informacje, a w konsekwencji na ich podstawie

przeprowadzone nieskuteczne operacje, powodują obniżenie efektywności pozyskiwania kolejnych istotnych danych rozpoznawczych. Udana operacja oczyszczenia z przeciwnika danej miejscowości powoduje zwiększone zaufanie ze strony ludności lokalnej do sił COIN i jej większą wolę współpracy. Uzyskane w ten sposób informacje pozwalają wyeliminować kolejnych członków opozycji, poprawiając tym samym bezpieczeństwo. Z kolei źle przeprowadzona operacja, bez odpowiedniego przygotowania informacyjnego, powodująca straty w mieniu czy śmierć ludności cywilnej, przyczynia się do wzrostu poparcia dla przeciwnika.

4. **Wszystkie operacje zawierają elementy rozpoznawcze.** Każdy uczestnik operacji bierze udział w aktywnym zbieraniu informacji m.in. poprzez swoje kontakty z lokalną ludnością, siłami bezpieczeństwa czy też przedstawicielami lokalnych władz. W związku z powyższym przed rozpoczęciem każdej operacji powinny zostać określone wymagania informacyjne (intelligence collection requirements).
5. **Informacje w COIN,** na które należy zwrócić szczególną uwagę, **przebiegają od elementów najniższego szczebla do wyższych struktur dowódczo-sztabowych**. Wszystkie szczeble dowodzenia produkują dane rozpoznawcze i jednocześnie je wykorzystują. Wynika to ze specyfiki konfliktu – sytuacja batalionów może być całkowicie inna podczas działań w różnych terenach. Jednostki szczebla taktycznego w wielu przypadkach nie posiadają wystarczających organicznych sił i środków rozpoznawczych. Powoduje to konieczność stworzenia systemu zapewniającego wsparcie tych jednostek przez elementy szczebla operacyjnego. W przypadku tradycyjnych konfliktów zbrojnych większość środków jest ulokowana na szczeblu powyżej brygady. W przypadku operacji COIN istotnym jest oddanie do dyspozycji dowódców szczebla brygady i batalionu części sił i środków pozwalających na samodzielne zbieranie i opracowywanie danych rozpoznawczych. Przykładowo w trakcie wojny w Iraku na szczeblu amerykańskiego batalionu marines trzykrotnie zwiększono sekcję rozpoznawczą. Posiadanie odpowiednich elementów rozpoznawczych na szczeblu taktycznym zapewnia szybki dopływ informacji do wojsk bezpośrednio w polu. W efekcie dowódcy operacyjni mają przegląd sytuacji w rejonie odpowiedzialności, natomiast jednostki walczące w polu otrzymują konieczne informację bez zbędnej zwłoki. W przypadku misji afgańskiej inne będą problemy w prowincji Herat czy Kunduz, a inne w prowincji Helmand. Ograniczenie się do wykorzystywania informacji uzyskanych przez elementy rozpoznawcze wyższego

szczebla wiąże się z ryzykiem przenoszenia niektórych wzorców z jednej prowincji do drugiej bez uwzględnienia lokalnej specyfiki.

6. **Jednostki wszystkich szczebli prowadzą swoje działania w złożonym systemie, w skład którego wchodzą elementy cywilne i wojskowe sił koalicyjnych oraz państwa gospodarza, a także elementy zewnętrzne.** W związku z powyższym wszystkie szczeble są zmuszone koordynować swoje działania rozpoznawcze z wymienionymi komórkami. Lepsze zrozumienie sytuacji i problemów na szczeblu lokalnym przekłada się na lepsze rozpoznanie na szczeblu regionalnym i narodowym. Wymaga to odpowiedniej synchronizacji na wszystkich szczeblach. Żeby to osiągnąć, ważne jest, aby na wszystkich szczeblach znane i zrozumiane były wymagania informacyjne dowódcy – PIR (priority intelligence requirements), dopasowane do danego szczebla[12].

Bardzo ciekawie przedstawił swoje doświadczenia z operacji COIN w Iraku gen. David H. Petraeus. W swoim artykule, zamieszczonym w „Military Review" w 2006 roku[13], wymienia on czternaście obserwacji:

1. Nie staraj się zrealizować za dużo tylko swoimi rękoma.
2. Działaj szybko, ponieważ armia wyzwoleńcza ma tylko połowę życia (później staje się armią okupacyjną).
3. Pieniądze to amunicja.
4. Zwiększenie liczby osób mogących skorzystać na nowym systemie jest warunkiem sukcesu.
5. Oceń rachunek „zysków i strat" przed każdą operacją.
6. **Rozpoznanie jest kluczem do sukcesu.**
7. Każdy musi się zaangażować w budowę społeczeństwa.
8. Pomóż budować instytucje, a nie tylko struktury bezpieczeństwa.
9. Znajomość kultury zwielokrotnia posiadane siły.
10. Sukces w COIN wymaga więcej niż tylko operacji wojskowych.
11. Definitywny sukces zależy od lokalnych liderów.
12. Pamiętaj o tzw. strategicznym kapralu i poruczniku.
13. Nie ma alternatywy wobec elastycznego i szybko adaptującego się lidera.
14. Najważniejszym zadaniem lidera jest ustanowienie odpowiedniego tonu i kanału komunikacji.

Co prawda gen. Petraeus wymienia rozpoznanie z nazwy tylko w punkcie szóstym: „Rozpoznanie jest kluczem do sukcesu", jeżeli jednak spojrzymy na pozostałe obserwacje, to widać, że ich prawidłowe uwzględnienie w operacji COIN jest niemożliwe bez odpowiednich informacji rozpoznawczych. W tak skomplikowanej operacji, jaką jest COIN, posiadanie aktualnych i użytecznych informacji jest istotne na każdym etapie.

Można posiadać ogromne zasoby finansowe, które źle wydawane mogą tylko przysporzyć przeciwników. Zrozumienie lokalnego systemu wierzeń, zależności rodzinnych i klanowych, a także zaszłości historycznych, wymaga ogromnego wysiłku analityków i innych specjalistów. W wielu przypadkach analityków takich należy szukać w środowisku cywilnym na długo przed zaangażowaniem się w konflikt. Konieczność budowania lokalnej administracji oraz potrzeba zaangażowania wielu lokalnych liderów wymaga szczegółowego rozpoznania środowiska, aby zakładane efekty zostały zrealizowane. Wreszcie konieczność zapewnienia szybkich i wiarygodnych informacji rozpoznawczych na każdym szczeblu dowodzenia stawia przed strukturami rozpoznania ogromne wyzwania, niespotykane w konwencjonalnych konfliktach.

INFORMACYJNE PRZYGOTOWANIE POLA WALKI – IPB

Niezwykle istotny w operacji COIN jest okres poprzedzający planowaną operację. Chcąc odnieść sukces, konieczne jest poznanie przeciwnika oraz zrozumienie wszystkich aspektów związanych ze środowiskiem konfliktu, na długo przed wysłaniem wojsk. Proces ten jest realizowany w ramach tzw. informacyjnego przygotowania pola walki, w skrócie – IPB (intelligence preparation of the battlefield).

IPB jest systematycznym i ciągłym (także w trakcie operacji) procesem zbierania i analizowania informacji na temat zagrożeń oraz środowiska w specyficznym rejonie geograficznym. IBP ma na celu wsparcie informacyjne dowódcy i sztabu w procesie planowania operacyjnego – OPP (operational planning process) oraz procesie podejmowania decyzji DMP (decision-making process). Prawidłowo przeprowadzony IPB pozwala w odpowiednim czasie i miejscu dobierać oraz maksymalnie efektywnie wykorzystywać posiadane siły i środki w zależności od wariantu działania przeciwnika – COA (course of action).

Jak już wspomniałem, jest to proces ciągły, realizowany zarówno przed planowaniem operacyjnym, jak i w jego trakcie, a także podczas prowadzenia samej misji. IPB musi być na każdym etapie zaktualizowany, ponieważ stanowi podstawę planowania kolejnych przedsięwzięć rozpoznawczych i operacyjnych. IPB realizowany przed rozpoczęciem operacji determinuje cały proces doboru i przygotowania wojsk do operacji. Źle przeprowadzony IPB spowoduje, że zostanie przygotowany dobry plan, ale dla złego przeciwnika[14].

IPB składa się zasadniczo z czterech części:

1. Zdefiniowanie środowiska konfliktu (define the battlefield environment).
2. Opis wpływu środowiska konfliktu na operację (describe the battlefield’s effects).
3. Ocena zagrożeń (evaluate the threats).
4. Określenie możliwych wariantów działania przeciwnika – COAs (course of action) oraz zagrożeń z tym związanych (determine threat COAs)[15].

Zdefiniowanie środowiska konfliktu

Na tym etapie istotnym jest zdefiniowanie środowiska konfliktu rozumianego jako obszaru geograficznego, warunków, okoliczności oraz czynników wpływających na zaangażowane siły i środki, determinujące ich zdolności operacyjne oraz wpływające na proces podejmowania decyzji przez dowódcę w rejonie operacji AOO (area of operation). Istotne na tym etapie jest

także określenia rejonu zainteresowania AOI (area of interest), który pomimo iż nie jest rejonem operacji, ma wpływ na sytuację tam panującą. Na przykładzie Afganistanu mogą to być rejony plemienne, które pomimo oficjalnych granic należą do Pakistanu. Rejon zainteresowania może być dużo większy w porównaniu do rejonu operacji i powiązany z nim szeregiem czynników, takich jak: rodziny, klany, religię, tradycję, linie komunikacyjne, zależności ekonomiczne, wpływ mediów na lokalną ludność czy zewnętrzne wsparcie finansowe i logistyczne.

Bardzo istotne jest, jeszcze przed przerzutem wojsk na teatr, ustalenie:

- struktur wojskowych i pozawojskowych zaangażowanych w COIN
- organizacji rządowych i pozarządowych państwa gospodarza
- organizacji międzynarodowych
- jednostek wojskowych sojuszniczych
- struktur zajmujących się zbieraniem i analizą informacji rozpoznawczych
- struktur i organizacji, z którymi należy w przyszłości wymieniać informacje oraz sposób ich wymiany.

Czynności te są istotne z uwagi na konieczność wspólnego działania na teatrze oraz interpretacji sytuacji w ten sam sposób[16].

Opis wpływu środowiska konfliktu na operację

Na tym etapie najważniejszym zadaniem jest zrozumienia środowiska konfliktu i jego wpływu na warunki prowadzenia operacji. Etap ten zawiera takie elementy, jak:

- środowisko cywilne, w tym: społeczeństwo, struktura społeczna, kultura, język, oficjalne i nieoficjalne władze, interesy i zależności
- geograficzna analiza terenu ze szczególnym uwzględnieniem: warunków terenowych, terenów wiejskich i miejskich, kluczowej infrastruktury oraz linii komunikacyjnych
- warunki pogodowe ze szczególnym uwzględnieniem: analizy warunków klimatycznych i pogodowych oraz wpływu pogody na aktywność ludności i przeciwnika.

Na tym etapie w operacji COIN najważniejsze jest odpowiednie zrozumienie środowiska cywilnego z uwagi na jego kluczowe znaczenie dla powodzenia całej operacji. Jeżeli weźmiemy pod uwagę środowisko afgańskie oraz jego złożoność, tj.: liczbę występujących

narodów, rodzaje używanych języków obcych, zależności klanowe i rodzinne, system wierzeń, historię oraz powiązania ze światem zewnętrznym – to łatwo zrozumieć, jak bardzo proces ten jest złożony i jakie w tym zakresie mogą wystąpić ograniczenia[17].

Ocena zagrożeń

Oceniając zagrożenia, należy zwrócić uwagę na zdefiniowanie i poznanie przeciwnika, jego możliwości oraz słabości, które dowódca może wykorzystać. W przypadku operacji COIN jest to trudne z uwagi na fakt braku jasnych struktur organizacyjnych przeciwnika oraz jego wyjątkowych zdolności adaptacyjnych do nowych warunków. Dowódca pomimo ograniczeń i trudności z uzyskaniem takich informacji będzie wymagał odpowiedzi na następujące pytania:

- cele oraz motywacje przeciwnika
- słabości struktur państwowych wykorzystywane przez przeciwnika
- formy i metody wykorzystywane przez przeciwnika w celu uzyskania poparcia ludności lokalnej
- organizacja sił przeciwnika, jego wyposażenie oraz stosowane formy i metody prowadzenia walki
- zidentyfikowanie przywódców wojskowych i politycznych oraz miejsca ich pobytu.

Z uwagi na częste powiązania z przeciwnikiem należy także zidentyfikować zagrożenia płynące ze strony zorganizowanego środowiska przestępczego oraz innych grup prowadzących działania przeciwko oficjalnemu rządowi[18].

Określenie możliwych wariantów działania przeciwnika COAs oraz związanych z tym zagrożeń

Celem tego etapu jest przeanalizowanie i określenie możliwych wariantów działania przeciwnika oraz taktyki, która może być zastosowana w trakcie ich realizacji. W pierwszej kolejności należy określić ogólne możliwe warianty działania lub ich kombinacje, a następnie określić taktykę przeciwnika w trakcie realizacji każdego z nich. Ważne jest także określenie warunków oraz okoliczności, w których przeciwnik będzie przechodził z jednego wariantu do drugiego[19].

RODZAJE ROZPOZNANIA

Generalnie źródła informacji możemy podzielić na dwie grupy: techniczne źródła informacji – tj. wykorzystujące techniczne środki rozpoznawcze, oraz osobowe źródła informacji – tj. wykorzystujące kontakty z ludźmi do uzyskiwania informacji rozpoznawczych.

W związku z ograniczeniami w objętości niniejszego artykułu autor skupił się na najistotniejszych technicznych źródłach informacji, a także szczegółowo scharakteryzował osobowe źródła informacji, które w operacji typu COIN odgrywają szczególnie istotną rolę. Do najistotniejszych technicznych źródeł informacji możemy zaliczyć:

TECHINT (Technical Intelligence) – rozpoznanie techniczne. Polega na uzyskiwaniu informacji rozpoznawczych poprzez analizę sprzętu, wyposażenia oraz środków bojowych przeciwnika. Analiza ta pozwala zrozumieć i ocenić możliwości przeciwnika, wykorzystywane przez niego techniki przy produkcji np. min-pułapek czy technologie do produkcji broni[20].

MASINT (Measurement and Signatures Intelligence) – rozpoznanie polegające na eksploatacji oraz analizie śladów pozostawianych przez przeciwnika. Pozwala rozpoznawać ukrycia przeciwnika oraz wykorzystywane przez niego drogi i linie komunikacyjne. MASINT jest także wykorzystywany przy realizacji operacji targetingowych[21].

GEOINT (Geospatial Intelligence) – rozpoznanie wykorzystujące dane obrazowe, przestrzenne oraz geograficzne w celu opisu oraz analizy geograficznej terenu. Produkty

GEOINT są bardzo skuteczne przy wykrywaniu dróg wykorzystywanych przez przeciwnika, możliwych miejsc ukrycia czy tras przemytu. GEOINT pozwala także na przygotowanie produktów wykorzystywanych w trakcie przemieszczania się w rejonach zurbanizowanych[22].

OSINT (Open Source Intelligence) – rozpoznanie oparte na ogólnodostępnych, jawnych źródłach informacji. OSINT jest bardzo przydatny dla zrozumienia sytuacji ogólnopolitycznej wokół konfliktu. Pozwala zrozumieć społeczny odbiór i postrzeganie zarówno działań powstańców, jak i sił COIN. W erze internetu OSINT pozwala także śledzić strony internetowe przeciwnika czy prowadzić z nim dialog za ich pośrednictwem[23].

OSINT jest integralną częścią działalności rozpoznawczej. Łatwość dostępu oraz zakres możliwych do zdobycia informacji pozwala strukturom rozpoznawczym przygotować odpowiedzi na wymagania informacyjne dowódcy PIR (priority intelligence requirements) bez użycia innych, bardziej wyrafinowanych technicznych środków rozpoznawczych. Studiowanie dostępnej literatury, środków masowego przekazu czy innych periodyków pozwala zrozumieć przeciwnika, jego strukturę organizacyjną, sposób postępowania oraz pozwala przewidzieć

jego kolejne kroki[24]. Uzyskane w ten sposób informacje po ich opracowaniu i przeanalizowaniu stanowią istotne uzupełnienie i poszerzenie informacji uzyskanych przy wykorzystaniu innych źródeł rozpoznawczych.

Wspominając OSINT, należy tu podkreślić dwa istotne wyrażenia: **otwarte źródło**(open source) oraz **publicznie dostępne informacje** (publicly available information). Otwarte źródło to osoba, grupa ludzi lub system zapewniający informacje bez intencji ich ochrony przed publicznym dostępem. Publicznie dostępne informacje to dane, fakty, instrukcje lub inne opublikowane informacje udostępniane na żądanie opinii publicznej lub dostępne w trakcie otwartych dla opinii publicznej spotkań. Najczęściej wykorzystywanym źródłami informacji w OSINT są: media, fora publiczne, dokumenty udostępnione opinii publicznej, informacje transmitowane przy wykorzystaniu internetu, TV czy radia, strony internetowe. Jednym z ograniczeń jest fakt, iż zakup opracowań czy książek oraz śledzenie wybranych stron internetowych może ujawnić zakres naszych zainteresowań[25].

Z roku na rok rośnie ilość informacji dostępna w internecie. Szacuje się, iż dostęp do sieci ma około 3 mld ludzi na świecie i ta liczba ciągle rośnie. Eksperci szacują, iż w 2007 roku było około 50 tys. stron internetowych (portale społecznościowe, blogi, strony z materiałami wideo itp.) prowadzonych przez różnego rodzaju ugrupowania terrorystyczne czy ekstremistyczne. Dla nich internet stanowi świetny kanał łączności pozwalający na dotarcie do potencjalnych zwolenników z przekazem informacyjnym, jednocześnie zapewniający anonimowość.

W operacji COIN, gdzie człowiek jest w centrum zainteresowania, OSINT zyskuje na znaczeniu. Środki masowego przekazu w tego typu operacjach są kluczowe dla odpowiedniego przekazu propagandowego zarówno przez siły koalicyjne, jak i przeciwnika. W operacjach typu COIN, jak w Afganistanie, sekcje zajmujące się OSINT muszą posiadać nie tylko specjalistów analityków, ale przede wszystkim specjalistów znających doskonale kulturę, język oraz wzajemne zależności w społeczeństwie.

OSINT ma także duże znaczenie dla budowania zaufania pomiędzy różnymi aktorami w rejonie operacji, jak: sojusznicy, organizacje pozarządowe, międzynarodowe organizacje pozarządowe czy struktury państwa gospodarza. Raporty czy analizy przygotowane w oparciu o ogólnodostępne jawne źródła informacji można wymieniać z innymi strukturami, nie łamiąc ograniczeń występujących w przypadku informacji niejawnych[26].

SIGINT (Signal Intelligence) – rozpoznanie sygnałowe. Bardzo skuteczne źródło informacji, wykorzystywane dla rozpoznania lokalizacji przeciwnika, jego planów, morale oraz możliwości. SIGINT jest bardzo istotny przy potwierdzaniu informacji uzyskanych od innych źródeł informacji, jak HUMINT[27]. SIGINTwykorzystuje w swojej działalności dane uzyskane poprzez analizę środków komunikacji przeciwnika – COMINT (Comunication Intelligence), promieniowania elektromagnetycznego – ELINT (Electromagnetic Intelligence), oraz emisji elektromagnetycznej – FISINT (Foreign Electromagnetic Emissions). Wymienione COMINT, ELINT oraz FISINT stanowią podkategorie SIGINT. Można więc stwierdzić, iż SIGINT uzyskuje informacje rozpoznawcze na podstawie analizy przechwyconej komunikacji przeciwnika, pozwalając jednocześnie na zlokalizowanie źródeł emisji[28].

IMINT (Imagery Intelligence) – rozpoznanie obrazowe, wykorzystujące dane uzyskane z analizy zdjęć fotograficznych, promieniowania elektromagnetycznego, promieniowania cieplnego czy danych pochodzących z radarów[29].Rozpoznanie to, wykorzystując środki techniczne (głównie platformy latające), pozwala lokalizować przeciwnika oraz wykorzystywaną przez niego infrastrukturę. Pozwala także śledzić jego ruchy, wykorzystywane linie komunikacyjne czy linie zaopatrzenia w ludzi i środki bojowe. Porównywanie zdjęć wykonanych w tym samym miejscu pozwala zaobserwować zmiany w infrastrukturze. Środki IMINT są szczególne przydatne w przypadku realizacji targetingu, umożliwiają także uzyskiwanie informacji i realizację operacji w rejonach zdominowanych przez przeciwnika. W trakcie operacji platformy latające, przekazując bieżący obraz, pomagają w kierowaniu operacją z centrów dowodzenia znacznie oddalonych od miejsca operacji. Pozwalają one maksymalnie wykorzystać posiadane siły i środki, jednocześnie ograniczając straty po stronie ludności cywilnej[30].

W warunkach afgańskich czy irackich przeciwnik wykorzystuje swoje atuty związane z perfekcyjnym wtapianiem się w otoczenie. Siły koalicyjne mają duży problem z jednoznacznym i szybkim rozpoznaniem przeciwnika pozwalającym na skuteczne i bezpieczne dla otoczenia operacje. W takich sytuacjach bardzo przydatne są bezpilotowe środki latające UAV (unmanned aerial vehicle). Ze względu na swoje możliwości techniczne są one niezwykle przydatne w szeregu misji, takich jak: zbieranie informacji o rejonie przyszłej operacji (IPB), prowadzenie rozpoznania przeciwnika, wykrywanie i śledzenie potencjalnych celów, bezpośrednie wsparcie walczących żołnierzy, ciągłe monitorowanie aktualnej sytuacji na teatrze, koordynacja i wskazywanie celów dla innych statków powietrznych, a także

bezpośrednie zwalczanie wytypowanych celów w przypadku misji targetingowych czy wsparcia wojsk. W przypadku targetingu nie do przecenienia jest możliwość identyfikacji celu i jego ciągłe monitorowanie, aż do chwili likwidacji. Możliwość bezpośredniej obserwacji pola walki pozwala osobom funkcyjnym na podejmowanie decyzji o wykorzystaniu danej broni, rozpoczęciu operacji, a także na ocenę ryzyka danej decyzji. Wykorzystanie UAV pozwala na prowadzenie aktywnych działań kinetycznych w rejonach, w których w danym momencie brakuje odpowiednich sił lądowych. Jednocześnie ze względu na swój zasięg, trudną wykrywalność oraz możliwości bezpośredniego ogniowego oddziaływania, UAV paraliżują swobodę działania przeciwnika w rejonach, nad którymi teoretycznie posiada on kontrolę. Odpowiednie wykorzystanie UAV pozwala na prowadzenie skoordynowanych lądowo-powietrznych operacji. Nie należy także zapominać, że UAV jest doskonałym źródłem informacji wykorzystywanym do potwierdzania lub poszerzania informacji rozpoznawczych uzyskanych przez inne źródła rozpoznawcze. Można pokusić się o stwierdzenie, że także w przypadku operacji typu COIN środki powietrzne odgrywają kluczową rolę[31].

G2X

G2X jest centralną strukturą sztabową koordynującą wszelkie zagadnienia związane z rozpoznaniem osobowym – HUMINT, i kontrwywiadem – KW. Koncepcja 2X rozwinęła się na podstawie doświadczeń amerykańskich zdobytych w trakcie konfliktów w Somalii, Haiti oraz na Bałkanach. W trakcie tych konfliktów pojawiła się koncepcja scentralizowania wszystkich elementów zajmujących się pracą z osobowymi źródłami informacji w strefie operacji w ramach jednej komórki[32]. Początkowo według teoretyków działaniami KW i HUMINT miała kierować jedno- lub dwuosobowa sekcja. Jednakże na podstawie kolejnych doświadczeń 2X rozszerzył swoją strukturę do trzech zasadniczych komórek, tj.: sekcji koordynacji kontrwywiadem – CICA (CI coordinating authority), sekcji operacyjnej HUMINT – HOC (HUMINT operations cell), i sekcji wsparcia – OSC (Operations Support Cell). W przypadku sił amerykańskich sekcja 2X funkcjonowała na szczeblu dywizji i korpusu, natomiast jej liczebność i struktura pozwalały w pełni kierować działaniami wszystkich podległych elementów KW i HUMINT[33]. Dodatkowo w 2X występuje sekcja analityczna, która ma za zadanie analizę raportów HUMINT i KW w celu uniknięcia sytuacji, gdzie dwie informacje potwierdzające się nawzajem pochodzą od tego samego źródła informacji. Sekcja analityczna w ramach posiadanych baz danych poszerza także uzyskane informacje[34].

W trakcie ostatnich konfliktów zbrojnych rola HUMINT i KW została zauważona i doceniona. Szacuje się, iż w trakcie konfliktów w Bośni, Kosowie czy Afganistanie około 80% wszystkich informacji pochodziło lub pochodzi z tych właśnie źródeł. Wprowadzona koncepcja integracji, centralizacji oraz wspólnego zarządzania operacjami HUMINT i KW na teatrze, w ramach jednej sekcji 2X, obroniła się i w przyszłości zapewne będzie rozwijana. W Afganistanie Amerykanie przebudowali system obiegu wytwarzanych przez KW i HUMINT raportów rozpoznawczych. Celem było skrócenie do absolutnego minimum czasu od wytworzenia raportu do jego publikacji w sposób dostępny dla wojsk „w polu". Dzięki otrzymaniu przez 2X prawa publikowania raportów z pominięciem wyższych szczebli analitycznych udało się zmniejszyć czas od uzyskania informacji do jej publikacji w sieci niejawnej do sześciu godzin. Ominięcie szczebli pośrednich umożliwiło szybkie i skuteczne wykorzystanie zdobytych informacji przez wojska. Dzięki tak funkcjonującemu systemowi KW i HUMINT stały się kluczowymi elementami w procesie targetingu. System 2X pozwalał na uzyskiwanie aktualnych, dokładnych i możliwych do natychmiastowego wykorzystania informacji rozpoznawczych. Dzięki posiadaniu innych platform rozpoznawczych – jak SIGINT czy IMINT – można było większość informacji potwierdzić i poszerzyć. Centralizacja osobowych

źródeł informacji w ramach 2X umożliwia także ich szybkie ponowne zadaniowanie w przypadku takiej konieczności[35].

KONTRWYWIAD

W operacji COIN zadania KW można zdefiniować jako neutralizację zagrożeń wynikających z ofensywnej działalności struktur rozpoznawczych przeciwnika. Ogólnie można stwierdzić, iż kontrwywiad realizuje swoje zadania poprzez aktywne uzyskiwanie informacji, prowadzenie dochodzeń kontrwywiadowczych, operacje kontrwywiadowcze oraz analizę uzyskanych w ich wyniku informacji[36].

Do najważniejszych zadań KW w ramach G2X należą[37]:

- uzyskiwanie informacji oraz neutralizacja zagrożeń w zakresie: szpiegostwa, terroryzmu, sabotażu, działań wywrotowych oraz przestępczości zorganizowanej
- prowadzenie dochodzeń kontrwywiadowczych
- ochrona kontrwywiadowcza osobowych źródeł informacji (także źródeł HUMINT)
- prowadzenie rozmów z potencjalnymi źródłami informacji
- prowadzenie przesłuchań osób zatrzymanych i podejrzanych
- sprawdzanie lokalnych pracowników w ramach zatwierdzonych procedur
- prowadzenie operacji kontrwywiadowczych mających na celu zbieranie informacji charakteru kontrwywiadowczego.

W obecnych konfliktach daje się zauważyć brak zrozumienia dla działalności kontrwywiadu. W przeszłości, gdy brano pod uwagę ewentualność konfliktu konwencjonalnego, zakres zainteresowania kontrwywiadu zawierał się w angielskim skrócie TESSOC (Terrorist, Espionage, Sabotage, Subversion, Organize Crime, Civil, Unrest), który oznacza: terroryzm, szpiegostwo, sabotaż, działania wywrotowe, przestępczość zorganizowaną i niepokoje społeczne. Obecnie sytuacja zmieniała się diametralnie. Jeżeli spojrzymy na charakter konfliktu w Afganistanie to większość operacji przeciwnika zawiera się w wymienionej wcześniej definicji. Chcąc być konsekwentnym, należałoby stwierdzić, że to operacja afgańska jest problemem głównie kontrwywiadu.

Drugim podziałem wynikającym z braku zrozumienia zadań kontrwywiadu jest podział konfliktów na: konwencjonalny i asymetryczny, za który w mniemaniu wielu odpowiada 2X. Należy w tym miejscu podkreślić, że zasadniczą linią podziału pomiędzy kontrwywiadem

i HUMINT a pozostałymi rodzajami działalności rozpoznawczej jest rodzaj wykorzystywanych źródeł informacji. W przypadku IMINT, SIGINT, MASINT są to źródła techniczne, natomiast w przypadku HUMINT czy KW są to głównie osobowe źródła informacji.

Bardzo ważnym elementem realizowanym przez KW jest sprawdzanie lokalnej ludności – LEP (Locally Employed Persons), starającej się o pracę na terenie baz sił sojuszniczych. Zwany vettingiem lub screninigiem, proces ten ma na celu głównie ochronę sił i obiektów własnych przed rozpoznaniem przez przeciwnika. Sprawdzanie to jest dokonywane w oparciu o posiadane przez osoby kontrolowane dokumenty, informacje rozpoznawcze oraz rozmowę z osobą sprawdzaną[38].

HUMINT

Zdecydowanie jednym z najbardziej skutecznych sposobów zbierania informacji w COIN jest wykorzystanie HUMINT. HUMINT możemy zdefiniować jako proces zbierania informacji przez odpowiednio wyszkolonych operatorów, wykorzystujących osobowe źródła informacji.

Celem tej działalności jest zidentyfikowanie przeciwnika, a także jego intencji, struktury organizacyjnej, sił, możliwości, stosowanej taktyki oraz wyposażenia[39].

Wykorzystywanie HUMINT daje ogromne możliwości w postaci informacji, jednak niesie także zagrożenia. Przeciwnik, doskonale orientując się w formach i metodach stosowanych przez siły COIN, używa tej formy działalności do swoich celów. W trakcie misji w Iraku czy Afganistanie podstawione osoby przekazywały fałszywe informacje, których celem było: wprowadzenie sił COIN w rejon przygotowanej zasadzki, likwidację swoich wrogów wewnętrznych rękoma wojsk COIN, powodowanie strat cywilnych, rozpoznawanie taktyki sił COIN, realizowanie operacji przyczyniających się do spadku poparcia miejscowej ludności czy wywoływanie niepotrzebnych operacji powodujących zmęczenie sił lub ich odciąganie od innych istotniejszych zadań. HUMINT, obok KW, jest najlepszym elementem do prowadzenia operacji związanych z kontaktami z osobowymi źródłami informacji. Ze względu na specyfikę pracy ze źródłami osobowymi tylko odpowiednio przygotowani operatorzy HUMINT mogą prowadzić tego typu działalność. Pozostali żołnierze, rozumiejąc specyfikę HUMINT, powinni w miarę posiadanych możliwości i nawiązanych kontaktów wskazywać ewentualnych kandydatów na źródła informacji[40].

HUMINT realizuje swoje obowiązki poprzez taktyczne rozpytywanie, przesłuchania zatrzymanych, rozmowy z żołnierzami i cywilami po zakończonych misjach, kontakty łącznikowe, kontakty z osobowymi źródłami informacji, badanie zdobytych dokumentów – DOCEX (document exploitation), oraz badanie zdobytego wyposażenia – CEE (captured equipment operations)[41]. DOCEX wykorzystuje w swojej działalności zdobyte materiały w postaci: dysków, telefonów komórkowych, laptopów, wyposażenia osobistego czy dokumentów. Uzyskane w ten sposób dane rozpoznawcze są bardzo istotne, szczególnie w konfrontacji z danymi HUMINT czy KW. Często stanowią ich uzupełnienie, potwierdzenie czy też zaprzeczenie[42].

Odpowiednio zbudowana sieć osobowych źródeł informacji służy za oczy i uszy wojsk COIN i stanowi swego rodzaju system wczesnego ostrzegania przed ruchami sił opozycyjnych. Stanowi on zamiennik systemu rozpoznania i śledzenia wykorzystywanego w trakcie konwencjonalnego konfliktu. Najważniejszym atutem HUMINT jest to, że poza informacjami o strukturze czy lokalizacji przeciwnika jest w stanie dostarczyć informacji o jego intencjach i motywach działania[43].

Największym mankamentem pracy HUMINT jako źródła informacji jest czas potrzebny na efektywne rozpoczęcie pracy w terenie, na którym nie było wcześniej innych elementów HUMINT. Czas ten wynosi minimum 45–60 dni od chwili przemieszczenia na teatr[44].

Ogromne znaczenie HUMINT i KW zostało zauważone w operacji w Iraku. Wysyłane jednostki szczebla taktycznego posiadały typową strukturę na wypadek wojny konwencjonalnej z dużą liczbą technicznych środków zbierania informacji oraz bez organicznego KW czy HUMINT. Realizując swoje zadania, już na teatrze przeszkalały część ludzi, którzy prowadzili swoje działania jako operatorzy HUMINT czy KW. Tego typu przedsięwzięcia przynosiły dowódcom pozytywne efekty w postaci informacji o sieci przeciwnika, jego powiązaniach z ludnością czy wreszcie stanowiły podstawę dla przygotowywania operacji targetingowych[45].

ANALIZA

Samo zebranie informacji przez źródła informacji nie jest procesem wystarczającym. Najbardziej skomplikowanym procesem, konsumującym jednocześnie najwięcej czasu, jest analiza. W operacji typu COIN jednym z najważniejszych wyzwań stojących przed ludźmi odpowiedzialnymi za rozpoznanie jest odpowiednie usystematyzowanie uzyskanych informacji w postaci baz danych, a następnie ich analiza. Z uwagi na charakter uzyskiwanych danych (ogromna ilość danych osobowych oraz źródeł informacji) jest to proces bardzo skomplikowany.

Należy podkreślić znaczenie terminu „all source intelligence", który możemy przetłumaczyć jako proces analizy wszystkich źródeł informacji, tj. procesu syntezy i analizy informacji zdobytych przez wszystkie źródła. Można go zdefiniować jako proces zestawiania i wykorzystywania informacji i danych pochodzących ze wszystkich rodzajów rozpoznania w jeden końcowy produkt analityczny.

Pomimo występowania pewnych podobieństw pomiędzy przeciwnikiem w konflikcie konwencjonalnym a COIN rola rozpoznania w obu rodzajach wymienionych konfliktów różni się znacznie. W operacji COIN przeciwnik jest trudno rozpoznawalny, iluzoryczny, a czasami niemożliwy do odróżnienia od lokalnego społeczeństwa. Bardzo często przeciwnik działa w sposób zbliżony do działania zorganizowanych grup przestępczych. Tworząc podziemne struktury, rozwija je i dąży do opanowania całego obszaru pozostającego w polu jego

zainteresowaniu. Nie mając jasnych zhierarchizowanych struktur, jest trudny do rozpoznania. Nawet posiadając wiedzę na temat struktury jednej komórki, trudno ją na inne obszary. Podstawowymi technikami stosowanymi przez przeciwnika są: ograniczone akcje zbrojne, zamachy bombowe, porwania, zabójstwa i próby zastraszania lokalnej ludności. Ludność cywilna generalnie nie jest atakowana lub atakowane są tylko wybrane osoby. Najważniejszym celem jest pokazanie, że struktury rządowe nie są w stanie zapewnić bezpieczeństwa ludności cywilnej. W takiej sytuacji rozpoznanie jest zmuszone do prowadzenia działań zbliżonych do taktyki stosowanej przez policję kryminalną. Podstawowymi sposobami zbierania informacji na tym etapie są: zbieranie danych biometrycznych, odcisków palców, analiza zdobytych dokumentów oraz wyposażenia, analiza powiązań i kontaktów czy przesłuchania zatrzymanych. Analiza tych informacji oraz konieczność stosowania technik typowo policyjnych powodują, że praca analityka w COIN znacznie różni się od rozpoznania w wojnie konwencjonalnej[46].

Najważniejszym celem tych działań jest znalezienie odpowiedzi na następujące pytania:

- zdefiniowanie przeciwnika, jego wyposażenia, wzajemnych powiązań (także ze środowiskiem cywilnym)
- lokalizacja przeciwnika, wykorzystywanych ukryć sprzętu i uzbrojenia, źródeł finansowania oraz linii zaopatrzenia
- szczegóły dotyczące uzbrojenia oraz stosowanej taktyki
- możliwe miejsca kolejnych ataków
- słabości, niedoskonałości oraz rekomendacje odnośnie celów
- wspólna analiza i dyskusja na temat struktur przeciwnika oraz najlepszej strategii walki z nim
- efekty planowanych i zrealizowanych operacji przeciwko jego strukturom[47].

Analitycy, zmuszeni do szukania odpowiedzi na powyższe pytania, stosują wiele narzędzi i technik analitycznych. Podstawowymi narzędziami są posiadane bazy danych informacji, zawierające głównie informacje na temat istotniejszych incydentów z udziałem przeciwnika, a także programy i narzędzia analityczne. Niestety, już na tym etapie analitycy spotykają się z dużymi problemami wynikającymi m.in.: z różnego sposobu opisu zdarzeń w zależności od autora raportu; większość danych jest zapisywana, aby wspierać przyszłe operacje, a nie analityków; różnorakość baz danych czasami trudno dostępnych; zapisywanie tych samych

informacji przy użyciu różnego nazewnictwa; problemy z wymianą informacji pomiędzy różnymi strukturami wywiadowczymi[48].

W operacji COIN przed analitykami stoi ogromne wyzwanie nie tylko ze względu na wielorakość obszarów koniecznych do zanalizowania, ale przede wszystkim z powodu ciągle zmieniającego się otoczenia konfliktu oraz szybkości, z jaką zbrojna opozycja adaptuje się do nowych warunków. Nieograniczony dostęp do mediów oraz ogromna ilość dostępnych tam informacji jest także analizowana przez przeciwnika. Większość informacji medialnych o zdarzeniach czy istotnych „aktorach" jest przez niego przechwytywana. Na nieszczęście dla sił zaangażowanych w COIN wszelkie próby wprowadzania nowych rozwiązań są szczegółowo analizowane już na etapie procesu koncepcyjnego.

Pisząc o analizie, należy wspomnieć o różnicy pomiędzy danymi czy informacjami a produktem analitycznym. Wszystkie informacje po ich dostarczeniu przez różne źródła informacji, jak: G2X, SIGINT, IMINT, OSINT, są tylko informacjami, które wymagają „przepuszczenia" przez proces analityczny. Po dokonaniu ich syntezy i analizy – czyli ocenie ich wiarygodności czy wartości, porównaniu z innym źródłami, a następnie zestawieniu

w jeden spójny produkt dotyczący wybranego obszaru – stają się wartościowym produktem analitycznym. W nomenklaturze NATO informacje przed przeanalizowaniem określa się jako „information”, natomiast po ich analizie używane jest określenie „intelligence”[49].

Proces ten wymaga personelu odpowiednio przygotowanego i wykształconego pod każdym względem. Personelu posiadającego wiedzę na temat technik analitycznych, specyfiki poszczególnych rodzajów rozpoznania, ich słabej i mocnej strony, wiedzy na temat analizowanych faktów oraz wiedzy na temat wcześniejszej działalności przeciwnika, w tym stosowanych przez niego technik działania. Osoby zajmujące się analizą muszą także posiadać wiedzę na temat całego systemu dowodzenia, aby produkt przez nie przygotowany był odpowiedzią na wymagania informacyjne dowódcy oraz żeby tak sporządzone raporty mogły stanowić podstawę planowania kolejnych operacji.

Mówiąc o analizie, należy także wspomnieć o różnicy pomiędzy analizą aktualnej sytuacji operacyjnej (current operations intelligence) a analizą powiązań wzajemnych przeciwnika (network insurgency analysis). Analiza aktualnej sytuacji operacyjnej jest odbiciem aktualnej sytuacji operacyjnej zarówno taktycznej, jak i operacyjnej i zawiera: dane na temat przeszłej i obecnej działalności przeciwnika; analizę efektów aktualnie prowadzonych operacji; wsparcie informacyjne aktualnie prowadzonych operacji oraz przygotowywanie i dystrybucja meldunków o zagrożeniach.

Analiza powiązań przeciwnika zawiera informacje na temat:

- struktury organizacyjnej przeciwnika
- kierownictwa przeciwnika
- najważniejszych elementów jego organizacji
- możliwości oraz kierunków działania
- powiązań ze środowiskiem lokalnym.

Informacje te pozwalają dowódcy na:

- zrozumienie i wykorzystanie słabości przeciwnika
- przewidzenie jego kolejnych posunięć
- zrozumienie sposobu myślenia lokalnej ludności
- zapewnienie danych wykorzystywanych w procesie planowania targetingu.

Ten rodzaj analizy wymaga ogromnego nakładu czasu, energii oraz informacji dostępnych w bazach danych. Analitycy mogą potrzebować czasami tygodni czy miesięcy oraz wielu źródeł informacji, aby na ich podstawie przygotować raporty na temat struktury organizacyjnej, taktyki działania – TTP czy przywództwa sił przeciwnika. W tym celu dowódcy powinni wydzielić grupę analityków, którzy pozbawieni presji czasu wynikającej z aktualnej analizy sytuacji będą mogli się skoncentrować na działalności długoplanowej. Jednym z najważniejszych produktów możliwych do przygotowania są informacje na temat sposobu myślenia przeciwnika czy lokalnej ludności myśli, ich odbioru rzeczywistości i wynikających z tego konsekwencji dla przyszłości operacji COIN. Dane te mogą być z powodzeniem wykorzystywane w planowaniu operacji typu PSYOPS (operacje psychologiczne) czy INFO OPS (operacje informacyjne).

PODSUMOWANIE

Na zakończenie należy stwierdzić, iż prowadzenie skutecznego rozpoznania w operacji typu COIN nie jest proste i ma wiele ograniczeń, z których najważniejsze to:

1. Szeroki wachlarz wymagań. W przeciwieństwie do konwencjonalnego konfliktu nie wystarczy rozpoznać liczby czy położenia sprzętu i wojsk przeciwnika, których tu nie widać. Istotnym jest poznanie i zrozumienie wszelkich aspektów życia ludności, jej kultury i historii. Należy przeanalizować wszelkie zagadnienia ekonomiczne, związane z rozwojem infrastruktury czy budową demokracji.
2. Szeroki wachlarz wykorzystywanych źródeł informacji. W operacji COIN mamy do czynienia z ogromną ilością danych personalnych. Problemem jest zdobywanie informacji przez tysiące osób, sposób ich zbierania oraz katalogowania w sposób umożliwiający ich skuteczne wykorzystanie w każdej chwili.
3. Szerokie spektrum potencjalnych odbiorców produktów analitycznych. W operacji typu COIN mamy do czynienia z wielką ilością osób, które w swojej działalności potrzebują wiarygodnych i aktualnych informacji rozpoznawczych. Są to: siły koalicyjne, siły państwa gospodarza, prywatne agencje zajmujące się bezpieczeństwem, osoby zajmujące się planowaniem przedsięwzięć logistycznych, struktury zajmujące się pomocą humanitarną oraz rozwojem infrastruktury, media oraz organizacje pozarządowe. Problemem jest stworzenie systemu umożliwiającego sprawne i bezpieczne wsparcie informacyjne dla wszystkich wymienionych elementów.

4. Przepływ informacji z dołu do góry, a nie odwrotnie. W operacji typu COIN najważniejszymi odbiorcami informacji są elementy taktyczne, bezpośrednio zaangażowanie w prowadzenie operacji. Kolejne szczeble operacyjne powinny w taki sposób zaprojektować kanały komunikacyjne, aby wszelkie użyteczne informacje docierały bez zbędnej zwłoki.
5. Konieczność prowadzenia rozpoznania z uwzględnieniem aspektów prawnych. W operacji COIN najważniejsze działania rozpoznawcze prowadzone są pośród ludzi i to oni są głównym podmiotem ich działania. Wiąże się to z koniecznością zbierania dowodów prowadzenia działalności zbrojnej poprzez kolekcjonowanie dowodów typowych dla działalności policyjnej. Z uwagi na trudności w odróżnieniu ludności cywilnej od członków ugrupowań zbrojnych zebrane dowody mogą być jedynymi, na podstawie których dana osoba poniesie odpowiedzialność.
6. Brak jednolitego i scentralizowanego przeciwnika. W trakcie planowania i prowadzenia operacji w COIN należy wziąć pod uwagę wiele potencjalnych celów, którymi są różne ugrupowania zbrojne posiadające różną strukturę, narodowość członków, różne interesy oraz TTP. Przeciwnikiem mogą być także skorumpowani członkowie rządu państwa gospodarza, grupy przestępcze zajmujące się przemytem broni czy narkotyków a także osoby wpływowe, o innych niż COIN celach.

Zestawienie najważniejszych różnic w prowadzeniu operacji konwencjonalnej i COIN[50]:

	OPERACJA KONWENCJONALNA	COIN
IPB – Battlespace (środowisko konfliktu)	Warunki terenowe	Czynnik ludzki – demografia, klany, grupy etniczne, narodowość, kluczowi aktorzy/grupy/rodziny
IPB – Effects (efekt)	Politycy nie są głównym obiektem	Politycy są zawsze w centrum zainteresowania
	Liniowy	Asymetryczny (sieć komputerowa, media, wojna informacyjna, ludność)
	Wpływ pogody i terenu	Wpływ infrastruktury, struktur rządowych, bezrobocia, mediów
IPB – Threat (zagrożenia)	Siła oraz struktura jednostek przeciwnika	Sieć, powiązania wewnątrz grupy
	Funkcjonująca doktryna	Taktyka i techniki działania – (Tactics Techniques and Procedures – TTPs)
	Głównie elementy wojskowe przeciwnika, zidentyfikowane i stanowiące poważne zagrożenie	Nieregularne działania – konieczność zidentyfikowania zagrożenia występującego na styku

		elementów zbrojnych, ludności cywilnej i aktywnych i biernych zwolenników opozycji
IPB – COA (warianty działania)	Działania szablonowe związane z czasem i obowiązującą doktryną działania	Działania oparte na wzorcach postępowania determinowanych przez określone cele
	Scentralizowana struktura łączności i dowodzenia	Operacje prowadzone przez luźno powiązane samodzielne komórki przeciwnika
COLLECTION (pozyskiwanie informacji)	Koncentracja na sprzęcie i wyposażeniu	Koncentracja na kluczowych aktorach/sieciach powiązań i ludności cywilnej
	Krytyczne elementy zdefiniowane na podstawie znajomości struktury organizacyjnej	Krytyczne elementy zdefiniowane na podstawie analizy powiązań personalnych i określonych wzorcach postępowania
	Nacisk na efekt kinetyczny	Nacisk na niekinetyczny efekt
	Pozyskiwanie informacji zdeterminowane przez układ D3A (decise, detect, deliver and assess), tj. decyzja wyboru celu, lokalizacja celu, wybór i dostarczenie broni oraz ocena zniszczeń (BDA – battle demage assessment	Wysoki nacisk na ciągły kontakt wzrokowy w trakcie D2TDA (decise, detect, track, deliver, assess), tj. decyzja wyboru celu, lokalizacja celu, ciągłe prowadzenie/obserwacja celu oraz ocena efektu
	Operator (collector) na stanowisku stałym w dużej odległości od celu	Operator bardzo blisko celu lub w bezpośrednim z nim kontakcie
	Znaczny udział SIGINT i IMINT	Duże znaczenie HUMINT
	Wykorzystanie głównie wojskowych kanałów komunikacji	Wykorzystanie osobistych środków łączności (łączność komórkowa, pagery czy internet)
	Operacje prowadzone na podstawie informacji rozpoznawczych	Operacje prowadzone w celu uzyskanie informacji rozpoznawczych
	Wykorzystanie głównie narodowych organicznych środków rozpoznawczych	Wykorzystanie organicznych i sojuszniczych środków rozpoznawczych, wymiana informacji
	Wykorzystywanie jeńców wojennych oraz analiza przejętego wyposażenia	Wykorzystywanie zatrzymanych, analiza zebranych dowodów podobnie jak w przypadku dochodzeń kryminalnych

[1] http://dict.pl/dict_iso.
[2] W przedmiotowym artykule w odniesieniu do partyzantów czy powstańców będę używał określenia: przeciwnik.

[3] *Counterguerilla Operations*, FM 90-8/MCRP 3-33A, U.S. Marine Corps, 29 August 1986, s. 1–5.
[4] *Counterinsurgency*, FM 3-24, 15 December 2006, s. 1.
[5] Ibidem.
[6] Ibidem.
[7] Ibidem.
[8] *Counterguerilla Operations*…
[9] Ibidem, s. 1.
[10] L.S. Turner, D. Corbould, J.T. Adair, L. Hamel, *Optimizing Deadly Persistence in Kandahar: Armed UAV Integration in the Joint Tactical Fight*, „The Canadian Army Journal Volume", 13 January 2010, s. 124, www.armyforces.go.ca/caj.
[11] K. Teamey, J. Sweet., *Organizing Intelligence for Counterinsurgency,* „Military Review", September-October 2006, s. 24–25.
[12] *Counterinsurgency*…, s. 3–25.
[13] D.H. Petraeus, *Learning counterinsurgency, Observation from Soldiering in Iraq*, „Military Review", January–February 2006, s. 1–12.
[14] *Intelligence Preparation of the Battlefield*, FM 34-130, Washington, 8 July 1994, s. 1.
[15] Ibidem.
[16] *Counterinsurgency*…, s. 2–3.
[17] Ibidem, s. 3.
[18] Ibidem, s. 3-12.
[19] *Counterinsurgency*…, s. 3-20.
[20] Ibidem, s. 3–28.
[21] *Counterinsurgency*…, s. 3–29. Targeting możemy określić, jako proces typowania i niszczenia celów ważnych z punktu widzenia realizacji zakładanych celów operacji. W operacji typu COIN celami w zdecydowanej większości będą przywódcy ugrupować zbrojnych przeciwnik, a także uzbrojenie oraz infrastruktura przez niego wykorzystywana.
[22] Ibidem.
[23] Ibidem, s. 3–28
[24] B.G. Fast, „*Open Source Intelligence",* http://findarticles.com/p/articles/mi_m0IBS/is_4_31/ai_n16419797/?tag=content;col1.
[25] M.C. Taylor, *Doctrine Corner, Open Source Intelligence Doctrine*, „Military Intelligence Professional Bulletin", October-December, 2005, s. 2–14, http://www.fas.org/irp/agency/army/mipb/index.html.
[26] W. R. Draeger, *Take Advantage of OSINT*, „Military Intelligence Professional Bulletin", July–September,
39–44, http://www.fas.org/irp/agency/army/mipb/index.html.
[27] *Counterinsurgency*…, s. 3–28.
[28] *Intelligence*, FM 2-0, 17 May 2004, s. 1–8.
[29] Ibidem, s. 1–7.
[30] *Counterinsurgency*…, s. 3–28.
[31] L.S. Turner, D. Corbould, J.T. Adair, L. Hamel, *Optimizing Deadly Persistence*…
[32] L. Lacy, *Lessons learned: Army National Guard G2X in Bosnia*, http://findarticles.com/p/articles/mi_m0IBS/is_4_29/ai_112129344/.
[33] R. Bukowski, *Bridging the doctrine gap: a CI and HUMINT focused look at the transformation of MI doctrine*, „Military Intelligence Professional Bulletin", special issue 2008, s. 5–15, http://www.fas.org/irp/agency/army/mipb/index.html.
[34] L. Lacy, *Lessons learned*…
[35] R. Stallings, M. Foley, *CI and HUMINT Operations in Support of Operation Enduring Freedom*, „Military Intelligence Professional Bulletin", October–December 2003, s. 43–46, http://www.fas.org/irp/agency/army/mipb/index.html.
[36] *Intelligence*…, s. 1–11.
[37] R. Stallings, M. Foley, *CI and HUMINT* …
[38] Ibidem.
[39] *Intelligence*.., s. 1–6.

[40] W. Innocenti, L. Martens, D.E. Soller, *Direct support HUMINT in operation Iraqi Freedom*, „Military Review", May–June 2009, s. 49.
[41] Ibidem.
[42] *Counterinsurgency*…, s. 3–-29.
[43] Ibidem, s. 3–26.
[44] W. Innocenti, L. Martens, D.E. Soller, *Direct support HUMINT*…, s. 53.
[45] Ibidem, s. 48–56.
[46] W.L. Perry, J. Gordon IV, *Analytic Support to Intelligence in Counterinsurgencies*, „Rand Corporation",
2008, XI–XV.
[47] Ibidem, s. 36.
[48] Ibidem, XIX.
[49] D.L. Madill, *Producing the Intelligence from Open Source*, „Military Intelligence Professional Bulletin", October-December, 2005, 19-24, http://www.fas.org/irp/agency/army/mipb/index.html.
[50] D. Zeytoonian, *Intelligent design: COIN operations and intelligence collection and analysis*, „Military Review", September-October 2006, s. 31.